REMARKS/ARGUMENTS

This case has been carefully reviewed and analyzed in view of the Final Office Action dated 21 June 2007. Responsive to the Office Action, Claims 1-5, 8, 9, 13, 16, 17 and 19 have been amended to clarify the invention of the subject Patent Application. Additionally, Claim 18 has been cancelled by this Amendment. Therefore, Claims 1-17 and 19-22 remain pending in the subject Patent Application.

In the Office Action, the Examiner rejected Claims 1 and 16 under 35 U.S.C. § 103(a) as being unpatentable over Greenfield, U.S. Patent # 6,748,528, in view of Garay et al., U.S. Patent #6,839,436 (hereinafter "Garay"), and further in view of Wong, U.S. Patent Application Publication #2002/0146127. Claims 2-4, 13-14, and 17-18 under 35 U.S.C. § 103(a) as being unpatentable over Greenfield, in view of Garay, and Wong, and further in view of Dinsmore et al., U.S. Patent #7,043,024 (hereinafter "Dinsmore"). The Examiner further rejected Claims 5 and 18 under 35 U.S.C. § 103(a) as being unpatentable over Greenfield, in view of Garay, and Wong, and further in view of Dinsmore and Kasahara et al., U.S. Patent #7,080,255 (hereinafter "Kasahara"). The Examiner rejected Claim 6 under 35 U.S.C. § 103(a) as being unpatentable over Greenfield, Garay, Wong, and Dinsmore, in view of Briscoe, U.S. Patent Application Publication #2003/0044017. Claim 7 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Greenfield, Garay, Wong, and Dinsmore, in view of Akiyama, U.S. Patent Application Publication #2003/0002680, and Claim 8 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Greenfield, Garay, Wong, Dinsmore, and

Kasahara, in view of Hardjono, U.S. Patent #6,584,566. The Examiner further rejected Claims 9-12 and 20-21 under 35 U.S.C. § 103(a) as being unpatentable over Greenfield, Garay, Wong, Dinsmore, and Kasahara, in view of Perlman, U.S. Patent #5,455,865. Still further, Claims 15 and 22 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Greenfield, in view of Garay, and Wong, and further in view of Kasahara et al., U.S. Patent #6,788,788.

Before discussing the prior art relied upon by the Examiner, it is believed beneficial to first briefly review the method and structure of the invention of the subject Patent Application, as now claimed. The present invention is directed to a method of key-management in Distributed Sensor Networks. The method includes the step of storing a respective key ring including a plurality of individually selectable private keys in each sensor node of the Distributed Sensor Network prior to deployment of the sensor nodes of the Distributed Sensor Network. The private keys are randomly chosen from a common pool of keys. The key rings of at least a pair of the sensor nodes have a pre-defined probability of having at least one private key in common. The method includes the steps of deploying the plurality of the sensor nodes of the Distributed Sensor Network, and actuating at least one sensor node to discover at least another sensor node sharing the at least one private key to establish a secure communication link between the one sensor node and another of the sensor nodes. The method further includes the step of using the at least one shared private key for subsequent secure communication between the at least one sensor node and the other sensor node.

The step of storing a respective key ring includes the steps of generating a key space having a multiplicity of keys, and randomly selecting a pool of keys from said key space. Further, the steps of assigning a specific key identifier for each key in said pool of keys, and randomly selecting a number of the keys from said pool of keys to form said respective key ring for each sensor node, are included. The number of keys is probabilistically determined to provide the pre-defined probability of the pair of sensor nodes has at least one shared private key, and storing the specific key identifiers with the respective key ring in each sensor node.

From another aspect, the present invention is directed to a Distributed Sensor Network system. The system includes at least two sensor nodes. Each sensor node is pre-loaded prior to deployment thereof with a respective key ring including a plurality of individually selectable private keys that are randomly chosen from a common pool of keys. The key rings of at least a pair of the sensor nodes have a pre-defined probability of having at least one private key in common. Each of the private keys of said key ring having an associated key identifier stored in a corresponding sensor node. The system further includes means for searching for another sensor node included in each sensor node, where a plurality of said key identifiers are broadcast to search for other sensor nodes with a matching key identifier. The matching key identifier indicates the other sensor node has a private key in common therewith to establish a secure communication link therebetween.

In contradistinction, the Greenfield reference is directed to a method and system for establishing a secure socket layer protocol communication. As described with reference to Figs 2 and 3, and contrary to the instant invention, a client 20 includes browser software that includes a **public key ring** 32 for use in establishing secure communications with a server 22, 24, 26. The client 20 further includes a writable public key ring 38 into which public keys are received. The secure communication links 34 and 40 both require **public keys**. Secure communication is established by transmitting the public key fro the server to the client, for example, and not an identifier that is associated with the private keys that two nodes have stored therein.

It is respectfully submitted that public key encryption (asymmetric encryption) is significantly different from private key encryption (symmetric encryption). Due to the size and power limitations of a distributed sensor network, the high computational demand and greater storage requirements of a public key encryption scheme make it undesirable for use in such a system.

Thus, Greenfield fails to disclose or suggest prior to deployment of a plurality of sensor nodes of the Distributed Sensor Network, storing a respective key ring including a plurality of individually selectable private keys in each sensor node of the Distributed Sensor Network, the private keys being randomly chosen from a common pool, the key rings of at least a pair of the sensor nodes having a pre-defined probability of having at least one private key in common, as now claimed in Claim 1. The reference further neither discloses nor suggests actuating at least one sensor node to discover at least

another sensor node sharing the at least one private key to establish a secure communication link between the one sensor node and another of the sensor nodes, as now claimed. Still further, the reference fails to disclose or suggest at least two sensor nodes, each the sensor node being pre-loaded prior to deployment thereof with a respective key ring including a plurality of individually selectable private keys randomly chosen from a common pool, the key rings of at least a pair of the sensor nodes having a pre-defined probability of having at least one private key in common, each of the private keys of the key ring having an associated key identifier stored in a corresponding sensor node, as now defined in Claim 16. Further, Greenfield fails to disclose or suggest each of the sensor nodes having means for searching for another sensor node where a plurality of the key identifiers are broadcast to search for other sensor nodes with a matching of at least one of the key identifiers, the matching key identifier indicating the other sensor node has a private key in common therewith to establish a secure communication link therebetween, as now claimed.

The Garay reference does not overcome the deficiencies of Greenfield. The Garay reference is directed to a method of maintaining broadcast encryption in the presence of compromised keys. The broadcast encryption scheme utilizes symmetric key (private key) encryption, and thus one skilled in the art would not look to Garay for methods of selecting keys in the system of Greenfield, which uses public keys that are sent to the client machines (subscribers). Therefore, it is believed that the Examiner's combination

of Greenfield and Garay is improper, based on "hindsight" using Applicants' own disclosure as a "blueprint" for combining the references.

Arguendo, even if the combination is proper, Greenfield and Garay together still cannot make obvious the invention of the subject Patent Application, as now claimed. The method of Garay relies on two set of keys, a randomized broadcast encryption (BE) key scheme and a unicast key. Both the BE key scheme and the unicast key are for a secure communication link between the trusted server11 and the privileged subscribers (Col. 4, lines 28-46), which may be considered to correspond to the sensor-controller keys of the instant invention. Nowhere does Garay disclose or suggest using randomized private keys for subscriber to subscriber (sensor node to sensor node) secure communications. Further, Garay relies on the randomized broadcast encryption key generation scheme to provide key sets that are a cover free family to provide each subscriber smart card with unique keys, whereby there would be "a very high probability that it is impossible for m smartcards to over another smartcard" (Col. 5, lines 13-45). Whereas, in the present invention the probabilistically determination of the subset of keys for each sensor node (subscriber smartcard) provides a high probability (0.999) that any pair of sensor nodes will have at least one shared private key.

Thus, the combination of Greenfield and Garay fails to disclose or suggest prior to deployment of a plurality of sensor nodes of the Distributed Sensor Network, storing a respective key ring including a plurality of individually selectable private keys in each sensor node of the Distributed Sensor Network, the private keys being randomly chosen

from a common pool, the key rings of at least a pair of the sensor nodes having a pre-defined probability of having at least one private key in common, as now claimed in Claim 1. The combination further neither discloses nor suggests actuating at least one sensor node to discover at least another sensor node sharing the at least one private key to establish a secure communication link between the one sensor node and another of the sensor nodes, as now claimed. Still further, the combination of references fail to disclose or suggest at least two sensor nodes, each the sensor node being pre-loaded prior to deployment thereof with a respective key ring including a plurality of individually selectable private keys randomly chosen from a common pool, the key rings of at least a pair of the sensor nodes having a pre-defined probability of having at least one private key in common, each of the private keys of the key ring having an associated key identifier stored in a corresponding sensor node, as now defined in Claim 16. Further, the combination fails to disclose or suggest each of the sensor nodes having means for searching for another sensor node where a plurality of the key identifiers are broadcast to search for other sensor nodes with a matching of at least one of the key identifiers, the matching key identifier indicating the other sensor node has a private key in common therewith to establish a secure communication link therebetween, as now claimed.

The Wong reference does not overcome the deficiencies of Greenfield combined with Garay. The Wong reference is directed to a system and method for secure communications between wireless units using a common key in a cellular network. The fact that the communication takes place in a cellular network is distinguishing. For one

wireless unit 70, 80 to communicate with a second wireless unit 72, 82, they must each communicate with a wireless communication system (MSC) (74 or 84 and 86). Each wireless unit has it own unique root key from which its own session key CK_1, CK_2 is derived. The wireless communication system(s) generates a common session key CK_C and transmits that key to the first and second wireless units using their respective session keys CK_1, CK_2. The two wireless units can then securely communicate with each other using the common session key CK_C.

Therefore, contrary to the Examiner's interpretation, one wireless unit is not activated to discover at least another sensor node sharing said at least one private key, as now claimed. Quite the opposite, the disclosed pair of wireless units do not share a private key, the common key is subsequently broadcast to them. Further, nether wireless unit is activated to discover the other unit based on a key that is pre-stored in the units. Additionally the reference neither discloses nor suggests the wireless units have means for searching for another sensor node where a plurality of said key identifiers are broadcast to search for other sensor nodes with a matching of at least one of the key identifiers, the matching key identifier indicating the other sensor node has a private key in common therewith to establish a secure communication link therebetween, as now defined in Claim 16.

Hence, the combination of Greenfield, Garay and Wong fails to disclose or suggest prior to deployment of a plurality of sensor nodes of the Distributed Sensor Network, storing a respective key ring including a plurality of individually selectable

private keys in each sensor node of the Distributed Sensor Network, the private keys being randomly chosen from a common pool, the key rings of at least a pair of the sensor nodes having a pre-defined probability of having at least one private key in common, as now claimed in Claim 1. The combination of references further neither disclose nor suggest actuating at least one sensor node to discover at least another sensor node sharing the at least one private key to establish a secure communication link between the one sensor node and another of the sensor nodes, as now claimed. Still further, the relied upon combination of references fail to disclose or suggest at least two sensor nodes, each the sensor node being pre-loaded prior to deployment thereof with a respective key ring including a plurality of individually selectable private keys randomly chosen from a common pool, the key rings of at least a pair of the sensor nodes having a pre-defined probability of having at least one private key in common, each of the private keys of the key ring having an associated key identifier stored in a corresponding sensor node, as now defined in Claim 16. Further, the combination of references fail to disclose or suggest each of the sensor nodes having means for searching for another sensor node where a plurality of the key identifiers are broadcast to search for other sensor nodes with a matching of at least one of the key identifiers, the matching key identifier indicating the other sensor node has a private key in common therewith to establish a secure communication link therebetween, as now claimed.

As the Greenfield, Garay and Wong, in combination, fails to disclose or suggest the concatenation of limitations the form the invention of the subject Patent Application, as now defined in Claims 1 and 16, they cannot make obvious that invention.

It is respectfully submitted that Dinsmore reference is directed to a system and method for key distribution in a hierarchical tree. This disclosure is directed to a group key distribution in a tree based hierarchy whereby multi-user evictions can be handled efficiently. Ordinarily, a user eviction from a group typically requires key regeneration for the entire group and that is a expensive and inefficient operation. None of the aspects of the invention disclosed in the reference are relevant to distributed sensor networks, as these networks are neither group nor tree based or organized. Even the background keying schemes used by Dinsmore (LKH, Iolus, OFT, OFC, etc.) are not applicable to sensor networks, because they are extremely communication and energy intensive.

Further, as Dinsmore is directed to a symmetric key system, it is not combinable with systems using public keys like Greenfield, Kasahara '788, and Perlman. The public key systems of Greenfield, Kasahara '788, and Perlman are thus not pertinent to the private key system of the present invention.

The Briscoe reference discloses generation of sequences of keys at a source, encrypting data units and regenerating the key sequence at the receivers to decrypt the transmitted data. This scheme is typically used for multicast applications. Key identifiers are used to keep track of the specific keys used in sequences of linked keys. In contrast, the present invention uses "collisions" in broadcast identifiers to determine what

keys are shared between pairs of sensor nodes, and unlike Briscoe, no keys or chains of keys are ever generated either at the source or at the receiver of any transmission. Instead, the keys of the present invention are pre-distributed, "off-line", **before** the sensor nodes are ever deployed. No key generation process in linked sequences or otherwise is ever carried out, as in Briscoe. To do such would be too energy intensive in an energy starved device, such as a sensor. Thus, the Briscoe reference is not only in a vastly different field from that of the invention of the subject Patent Application, but has no possible applicability to distributed sensor networks, where energy and computational power are limited resources.

The Hardjono reference is directed to a distributed group key management system for multicast security. Thus, the reference is not directed to pre-distribution of keys. The reference is relevant to Dinsmore, and like Dinsmore, is not applicable to distributed sensor networks.

Accordingly, the various combinations of the aforesaid references fail to disclose or suggest the combination of limitations that form the invention of the subject Patent Application, as now defined in dependent Claims 2-15, 17, and 19-22, and therefore cannot make obvious that invention.

For all the foregoing reasons, it is now believed that the subject Patent Application has been placed in condition for allowance, and such action is respectfully requested.

If there are any additional fees necessary in this filing, the Director of Patents and Trademarks is hereby authorized to charge deposit account # 18-2011 for such additional charges.

Respectfully submitted,
FOR: ROSENBERG KLEIN & LEE

/David I. Klein/

David I. Klein
Registration No. 33,253

Dated: 21 December 2007

3458 Ellicott Center Drive
Suite 101
Ellicott City, MD 21043
(410) 465-6678
Customer No. 04586

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this paper is being transmitted electronically to the U.S. Patent and Trademark Office, Art Unit # 2135 on the date shown below.

For: ROSENBERG, KLEIN & LEE

/David I. Klein/ 12/21/2007
DAVID I. KLEIN Date